Privacy and Security Tiger Team
Draft Transcript
April 1, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Call, so there will be opportunity at the end of the call for the public to make comments, and a reminder, workgroup members, to please identify yourselves. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman? Gayle Harrell?

Gayle Harrell – Florida – House of Representatives
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Judy Faulkner? Dave McCallie couldn't make it. Neil Calman? He also is unavailable today. David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block? Alice Brown for National Partnership?

Alice Brown – National Partnership for Women & Families – Director HITP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Leslie Francis?

Leslie Francis – NCVHS – Co-Chair
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Adam Greene?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Lisa Tutterow? Joy Pritts? Josh Seidman, you're on. Did I leave anybody off?

W
We have Adam and David from OCR too.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, David Holtzman. Deven, I'll turn it over to you then.

Judy Faulkner – Epic Systems – Founder
Judy Faulkner.

Judy Sparrow – Office of the National Coordinator – Executive Director
Oh, good.

Deven McGraw – Center for Democracy & Technology – Director
Great. Hi, Judy.

Judy Faulkner – Epic Systems – Founder
Hi.

Deven McGraw – Center for Democracy & Technology – Director
Thanks, everybody for joining us on this call this morning. Thanks also to members of the public who are listening in. We have a comparatively shorter call than usual this morning, from 10:30 to noon. But we are continuing our—I almost want to call it a forced march, but that's probably not exactly accurate, but—we're continuing our effort to prepare a set of privacy and security policy recommendations that have implications for stage two of EHR certification. Again, focusing on those recommendations that are still policy in nature but that require or are best supported by technical functionalities. The reason of course why we're doing this is because of the time frames and the need to tee these up for appropriate consideration by the Standards Committee so that we can meet the stage two certification preparation timeline.

We had distributed to the tiger team members some draft materials back on Tuesday and what I did with those was to just cut and paste verbatim the recommendation language that was in those documents on to the slides that we're going to go through today. For any of you that had a chance to read those documents before the meeting, there isn't really any difference between what's on the slide and what was in the paper. I just realized that it would be easier for both the tiger team members and the members of the public who follow our calls if that text was visible on a slide, versus being on my computer screen.

That's what we're going to do today. We're going to try to get as far as we can on three topics: patient identification and authentication, which we spent a fair amount of time discussing on our last call; user provider authentication, which we've discussed on multiple calls but I hope that we can put that piece to bed. Then other areas of privacy and security for stage two of meaningful use. Hopefully, we will be able to spend a fair amount of time on this call on that topic as well as the other two.

Then we've got one more call scheduled before the April 13th Policy Committee meeting. So it's still quite possible that we will continue to need to do some off line work on getting the language just right so that everybody's comfortable with it and to try to use the limited time that we have on calls to have substantive policy discussions versus incremental wordsmithing issues, if we can do that. We have some really good writers on our tiger team, and it's always helpful to get the word edits from you all. But it's much more efficient from a time perspective if we can do that off line.

Does anybody have any questions about what we're going to do today? All right, hearing none, we'll move right into the patient access pieces and where we're dealing with identity and policies around identity and authentication for patients seeking to access information in an EHR such as through a portal, which right now is being considered as part of the meaningful use stage two criteria in the patient engagement categories.

What we had said on our last call was that we recognize that the HIPAA security rule already places obligations on covered entities to implement policies and procedures for granting access to electronic protected health information. Given that, we concluded on our last call that we supported entities making these determinations based on their own assessments of what's necessary to address the risks of inappropriate access, but we wanted to support a series of principles that we would recommend guide those decisions about identity.

So here's where I tried to articulate some of the points that were made on our last call, including managing the risk of inappropriate access, but not setting the requirements in a way that discourages or inhibits patients from participating. Having the option to offer registering for access during an office or facility visit, but not necessarily making in person identification a requirement, because that might make it difficult for people who have difficulty getting into the office. I'm just going to go through all of these and then open up the call for a discussion. Talking about the point that Leslie Francis made, about when you are using identification methods that require people to answer questions and provide information, they need to be careful to choose information that's beyond basic demographics that might be known or knowable by an unauthorized person.

This point on D, which is requiring more stringent proof of identity for access to actual identifiable data in the EHR was my attempt to get at Neil's provisional point. Where people might be using a portal to do fairly, I would call them benign activities, but they're activities that don't really actually access the patient identifiable data, such as signing up for an appointment, those types of activities may not need the same stringent identity proofing. I don't know if I got that right, but that was my attempt to get at that point. Providers should consider the populations that they serve in setting their identification requirements.

Then the last one I threw on there was based on the feedback that we got from the VA, where they consult regularly with veterans to get feedback on what works from an identity perspective, and they've made some tweaks to the identity processes in response. So this last recommendation here urges providers to consider consulting patients to get feedback. Then, the last recommendation that I put up here, where I've got some sort of bracketed language suggestions that there ought to be some guidance provided to providers on trusted ID methods. That maybe that guidance ought to be updated to reflect what's going on in the federal government on e-identification, such as the National Strategy for Trusted Identities in Cyberspace.

With that, I'm going to stop and ask for feedback on this.

Paul Egerman – Software Entrepreneur
Deven, I just want to tell you I'm on the call.

Deven McGraw – Center for Democracy & Technology – Director
Oh, terrific. Thanks, Paul.

Paul Egerman – Software Entrepreneur
Sorry I'm a few minutes late, another call ran over, but I'm here.

Deven McGraw – Center for Democracy & Technology – Director
That's understandable. I actually forgot to double thank the members of the team who are pulling double duty on other workgroups that have been meeting quite frantically over the last week or more, because we very much appreciate your time and know that it's being tapped for numerous activities. And I would count you among that, Paul.

Leslie Francis – NCVHS – Co-Chair
Deven, I wanted to say that I think you've done a wonderful job of capturing the last discussion.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Well, thanks.

Alice Brown – National Partnership for Women & Families – Director HITP
I'll jump on the praise bandwagon. I also wanted to give a particular shout out, so to speak, ... the consulting of patients with respect to these identity procedures, whether it be a patient advisory group or even more routine day-to-day on the spot asking patients how this is going for them, and I think it can be an ongoing adjustment process if necessary.

Deven McGraw – Center for Democracy & Technology – Director
Okay. We can make it clear that a patient advisory group is one option, or even take that out. We're really just talking about getting feedback.

Alice Brown – National Partnership for Women & Families – Director HITP
Right, exactly, which I think is a great idea.

Deven McGraw – Center for Democracy & Technology – Director
Did anybody else have any suggestions for something that we forgot to include, a major issue with one of the points that we've made?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Again, like everybody else I'm in awe of the job you did in capturing this. You had some concerns about capturing Neil's input on contingent patient access, and I believe it's worth noting that the use case that he was particularly strong in talking about was patient input pre-appointment. I think the point he was making is that this is not necessarily an opportunity for a patient to learn what's in the system about him, but it's an opportunity to put information in the system. It's really valuable to get that before the appointment, so it's worth having a special contingency for that ....

Deven McGraw – Center for Democracy & Technology – Director
Do you know what, I had completely forgotten about that example, and we should specifically add that, I think. Anybody else?

Judy Faulkner – Epic Systems – Founder
Somewhere down the line, and I do think in the future biometrics, even though we had concern about them when we discussed them, I do think that that will become more and more appropriate. Suppose you have face recognition and even though your twin might be having the same face as you do, for most people if they have a choice they may say no, but ... the time they will click ... I'd just as soon that it does that. I do think they're going to be built into our software and hardware systems in the future, so I don't know whether we want to mention that in the future, or just avoid it.

Deven McGraw – Center for Democracy & Technology – Director
Maybe the point is, rather than calling out specific types of technologies that we suspect might become in more widespread use in the future, to maybe make the point that's on really recommendation number two on the slide that's up right now. About how the guidance, it needs really to be updated to reflect innovation and where the markets are going, and not just the fact that there is currently a federal

government focus on e-identification efforts, that the idea is to have the healthcare providers be evolving in this space just like pretty much everybody else does.

Judy Faulkner – Epic Systems – Founder
Yes, I think that would be great, because I would bet that it's going to evolve.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, and I would add innovation not unique to healthcare. The case Judy describes is a case where we rebalance the benefit of being guaranteed unique with other benefits in the process. Those propositions can easily be tested in banking or insurance or other places and really become understood and accepted by the public without having to have it developed exclusively in healthcare.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd like to make one comment. First, I really like the idea of adding something about how the methods will evolve over time. But I would also point out that biometrics are rarely used for identity proofing. They're used for authentication of that identity.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think, again, we don't want to call out and try to be crystal ball predictors, even though we have some really good technologists who have done quite well in doing that to say which is which. I think you're right, you'll notice when we get to the authentication slides that we try to make the same point there as well and I think we should similarly make sure that it's framed that the guidance needs to reflect the evolution in both identity and authentication technologies, both in and outside of healthcare.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I totally agree with authentication in particular, yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I don't know if we've imposed this particular aspect in this discussion, but we have to worry about shelf life on some of this stuff too. Unfortunately, the rate of the adoption of some of these technologies will make them cost prohibitive for providers to be able to implement, which is a concern of mine. The solution du jour of the year, a provider can't keep going and paying for and adopting new technologies constantly in order to provide these types of services and that concerns me. The same thing with fees and otherwise, we have to impose some type of reasonable limits on what we expect in terms of budgets and in terms of turnover of technology.

Deven McGraw – Center for Democracy & Technology – Director
Well, of course you do. I think that's why it's framed in terms of guidance and not necessarily— I think we're trying very hard not to establish a set of requirements in this particular space that we think are out of reach or potentially not doable by this industry even if they might be in widespread use in other industries, and in particular if they're not. We haven't recommended anything specific on here, and what we're suggesting is guidance not the imposition of new requirements per se.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
It just seemed like there was a lot of discussion about this evolution that's going on, and my fear is that evolution and technology can be so rapid that, again, what people might think is state of the art today in two or three years is not. I'm fearful that you could really spend an enormous amount of money on these types of technologies and forever be replacing them. I don't know what the answer is. I'm just raising the thought.

Deven McGraw – Center for Democracy & Technology – Director
As a person who feels like she buys a new computer every year, and I'm not also trying to run a facility, I actually personally feel a little bit of that pain.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's exactly why, though, that we have recommended annual risk assessments, because they shouldn't have to be doing this every minute. But annually they should reexamine their risk and reexamine what they need to address it, and that should take care of that.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But, Dixie, annual sounds like an awful long time for some people. But in terms of technology adoption and in terms of justifying cost and things like that, annual review, frankly, is an incredibly fast pace.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, I can tell you that all of the security technology we've discussed on this workgroup has been around for at least a decade, so I think if we get annual within healthcare we'd be real lucky.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I want to distinguish between the appearance and the adoption of the technologies. We see new technologies in biometrics come about. I don't think we go three months without some announcement of some tweak that changes it. The actual adoption across all industries is gated by the kinds of practical concerns that John is describing. Three years ago I got a laptop with a fingerprint reader on it and advice from the tech support person who gave it to me: "Don't use it." So I took his advice. The reason was not that the technology didn't work, but that if some ... happened, the machine had to go back to China to be rebuilt or something. The question of annual assessments does not equate to annual changes in technology.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, that's exactly right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think it's important to recognize that for all kinds of other reasons, not just the specifics of how patients are being authenticated, annual assessment is a very valuable thing to ask. After an initial assessment, annual updates are not necessarily the same trauma that the first assessment is. So I would say that the way Deven has positioned this covers us on the issue of not advocating a policy of adapting the newest nose hair identification as soon as it comes along, but I would not want us to take a position that was against annual assessment of security overall.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I don't disagree with that. I run a very large security organization. I understand the idea of annual assessments. I just think that we need to be incredibly careful that whatever technologies and proposals we make have some timeless element that does not become so burdensome that it becomes an inhibitor to try to—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Timelessness in IT is something that healthcare is very good at.

Deven McGraw – Center for Democracy & Technology – Director
It's a point well made. I think it is something that we should always keep in mind. Moving along to authorization, again, we're still on the topic of patients accessing electronic protected health information through an EHR, we had talked again in our last call about allowing for single factor authentication as a minimum in this space. So what I have tried to articulate here with what I thought were the consensus conclusions that we had reached on the last call, that single factor should be a minimum, but as is always the case when you set minimums providers can go above that. Here I framed it as wanting to offer their patients additional security or providing additional security for particularly sensitive data. But also keeping in mind the same guidelines that we set out for identification so that you don't, again, get the

requirements and the bar set so high in this space as well that people really don't feel that they can participate. I threw in the complicated password example that, I can't recall who made on our last call, but I thought it was a good one.

Then for recommendation number two, this was a point that we spent a fair amount of time discussing, and that is that for certification it would be important, given that we're only recommending one factor off a single factor authentication user name and password for this particular set of activities. That there ought to be at least a technical capability to detect and block programmatic attacks, or attacks from a known but unauthorized person, and I've offered some examples here. I may not have gotten that right. So in other words, if you have the capability in the EHR then the providers have some options with respect to how they deploy technology supported password management programs. Then again I reiterated the point here about needing providers to have guidance, and I think this one would need to be similarly worded to capture the evolution and innovation points that we made under identification.

With that, I'll stop and get feedback on this.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I know we've discussed this, and I'm afraid I've lost track of how we dealt with it. But there is a DEA requirement for two factor authentication for—

Deven McGraw – Center for Democracy & Technology – Director
Yes, and we do actually call for the certified EHRs to be able to honor that, but it's just in a different section of the recommendations.

Paul Egerman – Software Entrepreneur
To be clear, this is the patient authentication too.

Deven McGraw – Center for Democracy & Technology – Director
Yes, that's right. Thank you, Paul.

Paul Egerman – Software Entrepreneur
The DEA relates to ePrescribing ... patient authentication.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks. I'm slapping myself on the top of the forehead right now.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, while I certainly agree that certified EHRs should do the auto log off or block out after a certain number of unsuccessful log ons, is that in—actually, I do think that that's in the certification. I was thinking about auto time out. I think the log on is, never mind.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Really, this is about not blocking access to the EHR as a whole, but again we're talking about the patient authentication aspects, so whether it's through the portal or through whatever mechanisms that a provider offers patients for EHR access. All right, wow, we're doing really well this morning.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it's early.

Deven McGraw – Center for Democracy & Technology – Director
Moving on to trying to tie up user provider authentication, so moving off of patient access to an EHR, such as through a portal, and moving back on to a topic which is near and dear to our hearts. We've talked a fair amount about this but we're still trying to close the loop language wise on what should be the recommendations for authentication of individual provider users of an EHR.

You'll recall, just to refresh our memories, that we had presented some of our initial findings to the Policy Committee at the last meeting, the one that was in March, and got some feedback from David Blumenthal encouraging us to pursue stronger baseline user authentication requirements that would be enforced as a condition of participation in the Nationwide Health Information Network. Now, of course, those conditions are the ones being developed in the governance rule that ONC is working on, and so we don't really know a whole lot about what that's going to look like, so we're operating in a bit of an unknown and unclear space here. But nevertheless, the way that we have framed this was to say that there ought to be more in authentication of users than just user name and password, and again we're encouraging the team to focus on remote access, where we think that at least two factors should be required. We've thrown out, for discussion on the call, a potential definition of remote access, which is access over a public network like the Internet. We should discuss this. We also should keep in mind that anything that we would recommend to the Policy Committee that would potentially end up in the governance proposed rule would also be subject to public comment. So whatever we determine here, there are going to be multiple opportunities for the public to weigh in on it, whether we've got it right with respect to two factors for remote access, what would be an appropriate definition of what is remote, etc., etc.

Having said this, what's in bold on your slide is the straw recommendation, but we've also got some explanatory material underneath. Which is acknowledging that while we wanted more than single factor, more than user name and password for remote access to an EHR, we were not comfortable saying thou shalt do NIST or DEA because of the stringency of the second factor requirement in each of those sets of recommendations. Similarly, we struggled with how to define remote access. We probably will continue to do so a little bit on this call, but we're still trying to do that, in part because, again, keeping in mind that our initial recommendations on digital certificates for entity level authentication, we really thought that entities ought to have the flexibility in terms of how they authenticate their individual users within their facility. Then similarly, we discussed whether, but never really completely nailed down, whether the Standards Committee should be asked to determine which are appropriate factors for two-factor authentication for this set of circumstances.

I'm going to pause and see if Paul wants to add anything, because I know certainly the two of us have had plenty of conversations about this and he has significantly helped us try to shape this.

Paul Egerman – Software Entrepreneur
I think you did a good job.

Deven McGraw – Center for Democracy & Technology – Director
Okay, thoughts?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I have a thought. I think that referring to physical structures in this day and age really is sort of meaningless. But I do think that most organizations that care about security, and most organizations, do have their own network. Even if it's just within a small office, you usually have your own network. So I think it would be better to refer to the entity's private network versus the public network.

Deven McGraw – Center for Democracy & Technology – Director
So in other words, you would define access as access that's not through the entity's private network?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. Even in my house, we have our own private network in here that's wired and wireless, and I think that's appropriate for just about any size healthcare entity.

Paul Egerman – Software Entrepreneur
Dixie, what we're talking about is access to the EHR.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, and I'm sorry I wasn't explicit. I was really talking about that second sub-bullet, where it says "versus access within the physical structure," just put "access from the entity's private network."

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Paul Egerman – Software Entrepreneur
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's all. I wasn't explicit there.

Paul Egerman – Software Entrepreneur
I didn't understand. Now, I understand. That's fine.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Other thoughts? Okay, we did this, excellent.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's Friday.

Deven McGraw – Center for Democracy & Technology – Director
We've got to have more meetings on a Friday. So moving on to the additional recommendations that we've teed up here, and again these should all look really familiar to you because we've noodled over them for quite a number of weeks here. But we just want to really make sure that we've got it right so we don't have to keep bringing them up again. I promise you, you won't see them again after this call. Again, reminding folks that these recommendations set a baseline. It doesn't mean that organizations and entities, we want to be clear that they are free to go further than this and particularly when they're talking about their own employees or their own staff and contractors versus patients, where we have to worry about setting the bar too high.

For sensitive, higher risk transactions, there might be an additional authentication of greater strength subsequent to initial authentication that might be required, as is already recognized with the DEA. This is really more of a placeholder to acknowledge that we've set a general baseline requirement here but we're reserving the right to go back and reassess this for particular use cases, and this is something that people felt was important.

Again, we want to make a note here that whatever policies the Nationwide Health Information Network comes up with, they need to be reassessed for consistency for other national identity efforts and technology developments. We might want to add some similar language here that we've had in some of the other categories that we've discussed today about taking account of innovation, both within the healthcare space and in other sectors.

We also would like for ONC to develop and disseminate evidence about the effectiveness of various methods for authentication and reassess the NW-HIN policies accordingly. This is in response to the themes of discussion around not really having a great evidence base on what really works well in terms of authentication. Then here is where, Wes, we make the point that because there is an ePrescribing requirement where if you're prescribing a controlled substance you do need to do two factor authentication in accordance with DEA rules, but certified EHRs should have the capability to support that, and that's where this recommendation is included.

I think, let me just peek ahead and make sure that we got through all of them. We did. Does anybody have any comments on any of the rest of these provisions?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I guess we are assuming that somewhere there's going to be a definition of what we mean by NW-HIN.

Deven McGraw – Center for Democracy & Technology – Director

Yes. We're adopting the same unclear definition that the NW-HIN Working Group was using.

Paul Egerman – Software Entrepreneur
Dixie, I agree, that would be very helpful. We also need direction on how to pronounce it correctly. Is it N-win or New-Hin?

Deven McGraw – Center for Democracy & Technology – Director
New-Hin. N-win. N-Hin.

Paul Egerman – Software Entrepreneur
Maybe there's a west coast pronunciation.

Deven McGraw – Center for Democracy & Technology – Director
All right, moving on, you all are doing so fantastic. I'm beside myself here. Now we're moving to the set of additional privacy and security policy recommendations that are related to proposed meaningful use stage two objectives that, again, require EHR functionality or technical standards for certification in stage two. We started very preliminarily to sketch out at least the universe of the areas that we wanted to tackle, but we didn't have really very much time at all to go into detail on these. Not all of this is new, though. In some respects, what we're doing here is taking some of our previous policy recommendations and almost underlining them and pointing them more clearly in the direction of EHR certification.

So, for example, just to move to the first recommendation that we have here, we have two in the category of policies to facilitate secure exchange of EPHI. The first one reminds the Policy Committee that we have already adopted a recommendation requiring digital certificates and so we're noting for the committee that there ought to be in certification testing the use of digital certificates for appropriate exchange transactions. Similarly, we've got to repeat here on the DEA rule, which is you've got to test these systems for compliance with the DEA rule, which requires two factor authentication. Paul, did you want to add anything before we open it up?

Paul Egerman – Software Entrepreneur
No.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Again, this is, in many respects, it's just underscoring recommendations we've already made. Does anyone have questions, clarifications, comments? The next set of recommendations is related to the work that we did on accurately matching patients with their health information. Here, we have a set of recommendations that are, again, underlining what we've already said and pointing to the Standards Committee with respect to work that needs to be done from a certification standpoint in order to support those.

Here, I've got a question about whether the requirement to enter patient demographic data as a meaningful use requirement applies to both eligible providers and eligible hospitals. We'll pin that down. It's not really a big deal because the certification process isn't different for EHRs, for hospitals and providers. So we'll clean that up. But I think I know we need to focus on, again, the articulation of what needs to be done from a certification standpoint in order to implement policies promoting accuracy and patient matching, again, that we have already cleared through the Policy Committee and gotten adopted.

So we've got in Subsection A the Standards Committee should identify the standard formats for data fields that are commonly used for matching patients, specify the standards that describe how missing demographic data should be represented during the exchange. We talked a bit about USPS normalization of addresses. We didn't necessarily want to make that a requirement, but we had asked the Standards Committee to consider whether that would be beneficial to improving matching accuracy and whether it should be added to those standards. Then of course, the stage two certification criteria should test that appropriate transactions are sent and received with the correct demographic data format and data entry sequences exist to reject incorrectly entered values. Paul, did you want to add anything to this?

Paul Egerman – Software Entrepreneur
No.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Again, it's all related to recommendations that we've already made, but it's almost like we're underlining them and using this opportunity to remind folks that those recommendations are on the table and need to be implemented. Does anybody have any comments for these? All right, terrific.

Moving right along, policies to promote EHR security: Here, we're reminded that it's one of meaningful use eligible providers and eligible hospitals are required to conduct a review of security risk analysis in accordance with the HIPAA security rule and implement security updates as necessary and correct identified security deficiencies as part of the risk management process. As we discussed in our last call, we wanted to recommend that this measure also be included in stage two of meaningful use, and so that's what we've articulated here. Now, what I've got teed up for us to discuss next, which we didn't have time at all on our last call to discuss, is whether we want to go to the next step of saying something more specific about implementing the security functionalities that are currently in EHRs or that we might ask to be added to EHRs if we want to do that. But before we move to that discussion did we appropriately articulate what our recommendation is with respect to the conducting or reviewing of security risk analysis for stage two? It's pretty simple. Okay, terrific.

Moving on to the question on the table, which is should the tiger team add a recommendation. There's an obvious typo on this slide, which means that there's a typo in the document, regarding implementation of EHR security functionalities, and we laid out in the paper what I think are four options, and not all of them are mutually exclusive necessarily. We're not necessarily required to just choose one.

Option one is to require that providers address how they will implement these functionalities as part of meaningful use for stage two. This is actually very similar, if not exactly the same. We put this recommendation out , and I say "we," I think at that point the workgroup was still the larger Privacy and Security working group that hadn't been trimmed to its tiger team fighting weight. But we did put this recommendation before the Policy Committee that as part of your security risk assessment you ought to address how you're going to implement what I call the security functionalities that are in your EHR, the encryption, the auto log off provisions, etc., and that was not accepted by CMS. They expressed a reluctance at that particular time to adding to what the HIPAA security rule already had in place, and as you know many of the provisions of the security rule that are addressable are the ones that are linked to some of these EHR functionalities. So, for example, encryption in the security rule is addressable, encryption at rest and in motion is addressable.

Now, that doesn't mean that it's optional, and we do have some folks on the phone from the Office for Civil Rights, Adam Greene, who joins us regularly, and David Holtzman, to help us work through this. It's not optional but you do have some flexibility. If implementing the provision would not be reasonable and appropriate, you can document that and you have the flexibility to implement an equivalent protection if one is reasonable and appropriate. This is explained in a little bit more detail in the document. So requiring that they address how they'll implement the functionalities is one option.

Another option is to rely on the Office for Civil Rights in enforcing the security rule and determining whether it's in fact reasonable and appropriate not to implement an addressable provision of the security rule if it's tied to a functionality that exists in your EHR. We'll talk about that in a minute because I think I have a more detailed slide on each of these. The third option is specifically requiring encryption at rest for data at rest, and we'll go into this in a little bit more detail. Then the fourth option, which I'll almost call the high-test option, is requiring implementation of a more full complement of security functionalities consistent with some recommendations that the Standards Committee Privacy and Security Workgroup had developed. So that's the universe of options.

The first one is, again, the one that just requires the eligible providers and hospitals as part of a security risk assessment to specifically address how they're going to implement security functionalities, again,

very similar to something that was teed up in PHI, but that at time CMS was not enthusiastic about doing. That doesn't mean we can't try again. Of course, we're not asking providers to necessarily submit this material but to attest that they've done it and then of course they could be required to produce the documentation if the regulators ask them to.

The second option—and I'm just going to put these all on the table because, again, they're not necessarily mutually exclusive but I think we'll have a better discussion if we think about how they play off and interact with one another versus taking them one at a time. As I mentioned, we're talking about whether we would, instead of requiring something additional in meaningful use, to rely on the HHS Office for Civil Rights, which has oversight over both the HIPAA and Privacy and Security rules, to interpret how this rule applies to users of certified EHRs. Adam has generously allowed us to remind folks about something that he said at the HIMSS annual meeting, which is that if you've got an entity that's managing a certified EHR system that has built in technical safeguards for the confidentiality, availability, or integrity of the EPHI, they're expected, under the security rule, to have those system safeguards in operation. That means, again, it is addressable but when you have those functionalities in your EHR the expectation is that you're going to be using them.

Then the third option is to require specific implementation of data at rest. This is one that you could foresee combining with, say, option number two. The reason why we highlighted this is, Paul and I, in discussions about what the issues are with the security breaches that have occurred since the breach notification requirement that went into effect about a year and a half ago, most of those breaches have been related to theft or loss. If in fact the data had been encrypted, there wouldn't have been a breach, and notwithstanding that you don't have to notify if you do encrypt, entities are generally not encrypting data. So we're putting before you the possibility of a recommendation to use the meaningful use criteria as a lever to get the providers and hospitals to encrypt data at rest in order to try to address this problem.

Paul Egerman – Software Entrepreneur
Deven, just to clarify one thing. When you said "theft" most of the reports it's not necessarily theft, it's lost media. It could be theft of a laptop, but it could also just be somehow media can't be found.

Deven McGraw – Center for Democracy & Technology – Director
That's absolutely right.

Paul Egerman – Software Entrepreneur
So if you look at lost media, and view theft as one aspect of lost media, I think lost media is a better characterization for a larger percentage of the—

M
Are we supposed to comment on these specific slides as you're going through them, Deven?

Deven McGraw – Center for Democracy & Technology – Director
I'm going to give you a second to do so in a second.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Paul, I think at least with respect to what we've been seeing in the breach report, it's about 51% of large breaches, so breaches over 500 individuals, is based on theft, and then loss comes in third. Theft has been the biggest. Theft and loss combined is about 66% of large breaches.

Paul Egerman – Software Entrepreneur
When I look at lost media, I include theft within lost media. In other words, to me one way or the other you don't know where the media is. It could be somebody stole it. It could be somebody lost it. It could be somebody lost it and claimed it was stolen. It's hard to know what happened there. I put those two together and maybe that's confusing because you keep those two separate. I view theft of media the same as lost media, you just don't know where the media is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Deven, this is Dixie.

Deven McGraw – Center for Democracy & Technology – Director
Can you hold on a second, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, I have a question about this one.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I just want to say that what we have for option four is the slide, Dixie, that your Privacy and Security Working Group of the Standards Committee had put together. Here it sets a higher bar and actually requires implementation of certain functionalities. But I don't want to go through these slides in any detail yet. I would like people to now be able to ask questions and talk about the different options on the table and which ones we might want to pursue. So, Dixie, go right ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, now I have two comments then. Regarding sub-bullet three, would this be encryption at rest regardless of whether the media is physically protected within the organization or mobile media?

Deven McGraw – Center for Democracy & Technology – Director
That's a good question. If we wanted to make a distinction in that regard we could. I think we have framed it as a requirement to specifically implement the encrypting data at rest. Paul, do you have a thought on that?

Paul Egerman – Software Entrepreneur
Yes, I do. Actually, what's written here for option three is not what I would have intended, because I don't think you can require encryption of data at rest, I think there are a lot of reasons, and I don't think that's what it means when it says to be addressable. I think what I was hoping we could do in stage two of meaningful use is that providers might attest that they've addressed the issue. So either they've done encryption of data at rest, or they've done whatever you're supposed to do to make sure that you take the right steps so that you don't have these problems with missing media.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
When you look at the implementation specifications for encryption, it says "implementing mechanisms to encrypt electronic health information wherever deemed appropriate." I think to Dixie's point, I have enormous databases within my data centers on SAN storage devices which are striped and the like, and they're not encrypted. However, for a variety of reasons we don't think we need to. There are performance implications. There are cost implications. But there's also the practicality of actually doing that and risk that there really isn't as much of a risk. As opposed to, I think when you talk about data at rest is if somebody has a laptop with data on it I guess physically that data's at rest on the laptop, but I think that is a different class of at rest maybe or a different class of state of something—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
A different risk profile, right.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Exactly. So I wouldn't even call data on a laptop or a USB drive as being at rest. The way I almost think of some of that is being in transit because it is more greatly exposed than if it's in my data center and sitting on one of my large systems.

Paul Egerman – Software Entrepreneur
The way I'd respond to that, John, is you started by saying, if I heard you right, you have these data center disks and they're striped and you've taken precautions so you don't think you need to do encryption. The way I look at it is, again, what I'm suggesting is slightly different than what's written on the screen, is as part of meaningful use you should just attest that you've done that.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Absolutely.

Paul Egerman – Software Entrepreneur
To me that's consistent with what the requirements are.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I would—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But obviously—

Deven McGraw – Center for Democracy & Technology – Director
Hold on, let John respond to that, Dixie, and then you can go.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I was as much responding to what Deven said earlier, which is that even though it's addressable it's a requirement that data be encrypted at rest. I just wanted to make sure that there was an understanding that it's not really a requirement that it be encrypted, but that based upon, as Dixie had indicated, based upon the threat factors we may decide we have to encrypt it. But it's a more complex analysis maybe than what we're making it out to be.

Paul Egerman – Software Entrepreneur
To put the issue differently, what you just said sounds great. In other words, to me the issue is not necessarily encryption of data at rest. What we'd like to do is make sure everybody's taking the right steps so we don't have this media problem, because that seems to be a major problem. It says it apparently in the revs or whatever that you're supposed to either encrypt it at rest or do something. So if what you're saying is your organization has done something, then that's the attestation. In other words, the idea is to increase the security bar in stage two of meaningful use to try to address the fact that we've got all of this stuff going on and we'd like to stop it with missing media.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
What you might be able to say, which I think is much more palatable, is in light of the Mass General agreement with OCR, which basically says that Mass General will encrypt data on USB drives.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Can I say something?

Deven McGraw – Center for Democracy & Technology – Director
Go ahead, Dixie. I'm sorry. I was just about to call on you. Go ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
First of all, I totally agree with, and I'm glad you and Paul came up with this. I think if anybody ever looked online at the breach notification database, it's astounding. I would say that what Paul is suggesting already is required, that's a HIPAA requirement, is encrypt where deemed necessary. They obviously are not doing that. But if you look at the database online you will see that, well, Adam just said, 66% are lost media or theft, you know laptops or desktop PCs. I think that it would be a reasonable stage two requirement to say you must encrypt data on media that are mobile or otherwise not physically protected, such as laptops, USB drives, smartphones, all of that where they're walking around carrying PHI. I think it's a reasonable stage two meaningful use requirement.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

That is consistent with, if you read the Mass General agreement it seems like that's where OCR is really going.

Deven McGraw – Center for Democracy & Technology – Director
So in other words, Paul, what do you think about that?

Paul Egerman – Software Entrepreneur
I think that part is okay. We need to be clear at this point, though, that we're talking about a meaningful use attestation situation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
Because there's not a way to reasonably do this from a certification standpoint. But it's more of an issue to policies that the entity has to establish. I think what you suggested, Dixie, is fine, although I guess I still want to suggest that we go one step further, because I'm saying there's also an issue with what goes on within these data centers. And either the data should be encrypted at rest, or they should do some attestation as to what they're doing as an alternative to make sure that it's not—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But they're already required to do that, Paul.

Paul Egerman – Software Entrepreneur
I understand. They're already required to do it on the mobile devices too. The issue I'm saying is by doing that we're just trying to emphasize the point and raising the bar because there are problems.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
In other words, is it right to frame it, I've gone back to option one in the set of slides, because this is where we did frame a recommendation that requires them to specifically address how they're going to implement security functionalities in the EHR. But we can re-frame this to focus on the encryption at rest aspects of it that are different from those that Dixie identified and that I did take notes on, that ought to be required.

Paul Egerman – Software Entrepreneur
Basically I think that's right. Basically what I'm trying to suggest we do is shine a spotlight on this area and even though it's redundant with the regulations, hopefully by shining this spotlight in the area we can get some level of improvement. So I'm not trying to create new requirements or new law. I'm just trying to specifically call out encryption at rest in mobile devices. So you either have got to do it for the mobile devices and you've either got to do encryption at rest for your data center, or you've got to say what steps you've taken to make sure that you mitigated the risk. It's the same as what the law says. In effect we're just emphasizing it in meaningful use stage two.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But so far we've been told, and Deven, you know why, I don't—

Deven McGraw – Center for Democracy & Technology – Director
I can't say that I do. I think generally the way – I didn't let you finish, Dixie. Go ahead. I ... where you were going and interrupted you. Sorry about that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, on the one hand we've been told we can't repeat something that's already the law, because the implication was that HIPAA's optional. I agree with what Paul is saying. I'm just trying to anticipate what we're likely to—

Deven McGraw – Center for Democracy & Technology – Director
I remember asking Tony Trenkle about this, about the language that was in the meaningful use stage one final rule about CMS being reluctant to use the meaningful use program as a way to advance privacy and security policies that were different from or in addition to what was in HIPAA. That was certainly their feeling at the time, but we're now further along in implementing the breach notification provisions. We know a little more about how the providers are responding to the incentives that already exist in the statute and the evidence is pointing in the direction of they're not responding to the incentives to encrypt and that we might try again. I guess worst case scenario it doesn't get accepted but we have certainly used our bully pulpit. One could argue we should use our bully pulpit to make this point again.

Paul Egerman – Software Entrepreneur
And also here's my argument as to why we want to use the bully pulpit, and my argument for Tony is that this specific issue we appear to have a compliance problem, because we have so many incidents. When these incidents occur they're frequently front page news for local news media. This is a big deal. When that occurs, unfortunately it undermines our adoption goals. It creates a lot of concerns on a lot of people. It would be nice not to do that.

Gayle Harrell – Florida – House of Representatives
Deven, I'd like to comment on that specifically. I couldn't agree with you more, Paul. I think that this is absolutely critical, because every time there's a breach you wind up with a public distrust of the whole system. It's particularly important when they see 10 million records in Virginia being stolen or whatever, people get very antsy about this, so I think the more we use our bully pulpit to restate things or put within the rules however you can do it to strengthen it. Make it so that people understand this is not optional, they have to do it.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Again, I don't think we're doing anything that's out of order right now because the resolution agreement with Mass General and the corrective action plan talks about laptop encryption and USB drive encryption as being required when people are moving data off site from Mass General now as part of that agreement. So this to me is telegraphing OCR's opinion as to what we need to do with respect to certain types of things like off-site movement of data, whether it be on a laptop, a USB device, or otherwise.

Gayle Harrell – Florida – House of Representatives
Deven, I have another question. How within that do you deal with the hacking issue? In our large data centers, I mean, certainly, there are security provisions there, but how would this address hacking?

Paul Egerman – Software Entrepreneur
It's a good question, Gayle, but I think that's a different issue. If you don't mind, I'd like to see if we can make sure we have consensus on this issue before we address that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Paul, I'd also like to say that your recommendation really does address that to a degree. I like your recommendation, and I think that we should take it forward. If we have to come back and revise it, we can.

Paul Egerman – Software Entrepreneur
Dixie, I want to be clear, my recommendation, though, is not limited to the mobile devices.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know. I know.

Paul Egerman – Software Entrepreneur

What I'm trying to do is I'm trying to zero in on all of the sources for this missing media. But I actually think it works to everybody's advantage, and again to speak to your point as to why Tony Trenkle or CMS should make an exception, it's because I think we have pretty good evidence that there's not good compliance with the regs right now and it's creating a problem for us.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
I've got a question, though, about the scope of meaningful use on this context, which is that meaningful use is focused on the EHR rather than protected health information more generally. Is information that's getting exposed that's on laptops, for example, or USB ports, is that part of the EHR or is that really that they've taken information from the system and downloaded it outside of the EHR and would therefore potentially fall outside of the meaningful use realm? Because I imagine if you've got a fleet of laptops you don't have each one of them filled with patient records, but rather there may be an ability to download the patient records and put them on a particular laptop.

Paul Egerman – Software Entrepreneur
It's a great question, Adam. I think the answer is a little bit all over the map; sometimes they're EHR data, sometimes they're not. It's also unclear where the EHR begins and ends. So you see situations where you have, and Gayle and I exchanged some e-mails about an incident that occurred in Massachusetts at South Shore Hospital, and what they had there was demographic data on patients and they had a lot of financial data, in other words, they had claim form data. So that's definitely protected health information, whether or not that's EHR data, I kind of think it is, but it's an interesting question.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
There may be a distinction between whether the recommendations are really aimed at encryption of files at rest, so specifically the EHRs, the functionality to encrypt any copies that it leaves behind, versus whole disk encryption of the laptop fleet, which may be really outside the scope of the meaningful use discussion.

Paul Egerman – Software Entrepreneur
That's right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think Adam makes an excellent point, that any kind of a certification or attestation recommendation about the EHR falls short of the total target. Nonetheless, if we have an opportunity to raise the issue and raise attention to it, it's worth taking that opportunity, even if we aren't able to create a policy recommendation that covers spreadsheets, for example.

Judy Faulkner – Epic Systems – Founder
We have to be careful not to mislead people also, because they may think it's safer than it is. We don't cover the labs. We don't cover all the other places that information is sent to. So people could think, oh yes, everything is safe, but it's sent all over the place.

Paul Egerman – Software Entrepreneur
Judy, you're correct, although what might happen, and I don't know for sure, to speak to what Adam was saying, is a lot of organizations just would end up encrypting all of their laptops because it's too hard to figure out which are the ones you want to do and which ones you don't want to do. That actually helps you because a lot of these labs—healthcare's not the only place where this problem occurs. The problem occurs with payroll systems, so people are losing laptops that have 30,000 payroll records on them and then having to contact people. So your comment's a good one, though. It's not going to solve everything. We're just trying to mitigate what is—

Judy Faulkner – Epic Systems – Founder

Oh no, I'm not against it. I just think we have to be careful not to mislead people that it will solve everything.

Paul Egerman – Software Entrepreneur
I think that's fair. If I hear you right, what you're saying is this won't eliminate the Wall of Shame, the nickname for what goes on right now, the Wall of Shame.

Judy Faulkner – Epic Systems – Founder
It won't eliminate it, and we should be glad of what we're doing but not make people think that everything is covered.

Deven McGraw – Center for Democracy & Technology – Director
Right, absolutely.

Paul Egerman – Software Entrepreneur
Okay.

Deven McGraw – Center for Democracy & Technology – Director
It sounds like what we're coalesced around is seeking a requirement to implement encryption for certain types of media, and we'll be able to wordsmith this on the last call, but mobile devices, laptops, USB drives, smartphones being among the list which you would. But then for encryption of data at rest in other formats such as on your server, what we're asking for is that eligible providers and hospitals would specifically address how they're going to implement encryption at rest.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I don't think that that's the case. I think what we talked about is whether we need it or not and how we would have an appropriate plan to secure that data. Again, I think a lot of organizations today will not encrypt data at rest within a data center.

Deven McGraw – Center for Democracy & Technology – Director
Well, I thought we were framing it as specifically addressing how they're going to implement that particular functionality—

Paul Egerman – Software Entrepreneur
That's right. There's—

Deven McGraw – Center for Democracy & Technology – Director
—... requirement per se.

Paul Egerman – Software Entrepreneur
It's not a requirement that you have to encrypt it at rest in a data center. For a data center, you would have to say something about why you've chosen not to increase it at rest and what you've done as an alternative to make sure the media is secure.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think that's what I was just trying to say. What Deven said was a plan for people to encrypt it in the data centers and I said that that's not always the case.

Deven McGraw – Center for Democracy & Technology – Director
Okay, sorry, I didn't explain that right. Good point, John, sorry about that. Thanks for the clarification, Paul. Dixie, I think that's a very powerful set of recommendations that we can put forth for meaningful use. Did we want to say anything else about any of the other implementation of any of the other security functionalities, such as setting up some specific requirements, requiring people to address them, which we know is already in the security rule? Or, are we comfortable looking to OCR to do what it does, which is to oversee implementation of the security rule, including the addressable requirements, and consistent with the latest statements that they've made, which is not formal guidance. But I think it's very hopeful

language about how assessment would be done of how somebody using a certified EHR system would be implementing those provisions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, could I just clarify that last bullet there?

Deven McGraw – Center for Democracy & Technology – Director
Sure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Or clarify, not the last bullet, but I was still looking at my own version of the last slide, clarify what we actually did. I know Wes knows what we did because he was part of it, but what the Privacy and Security group did was we looked at all of the HIPAA implementation specifications that were labeled addressable, recognizing what Adam said is absolutely right, they still have to address them. They're not optional. But they have to either do what the implementation spec says, or explain why what they did is better or appropriate. We looked at it from the perspective of given that all of these entities we're talking about have implemented electronic health records, or they wouldn't be there to begin with, does it change whether this requirement should be addressable versus required? Does the fact that they have ... EHR make it such that that should really be required? That's what you see on the slide and the next one. That's where it came from. It was exactly that exercise.

Deven McGraw – Center for Democracy & Technology – Director
But you're suggesting that it should be required rather than addressable?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. For example, termination of system access of terminated workforce members, given that they have an EHR we think, yes, that should be required instead of just, well, I didn't have to do that because I don't have an EHR. So that's the thought process that went into this.

Deven McGraw – Center for Democracy & Technology – Director
Help me then, Dixie, understand because since ONC doesn't implement the security rules, nor does CMS, and so they don't really have the authority to dip into the security rule and make them required, how would that translate to stage two of the financial incentive program?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It would have to be part of the attestation. That feeds into whether CMS would be willing to go along, but they would have to attest to, yes, I have a process for terminating system access immediately when workforce members leave. It would still be attestation, you wouldn't send OCR out there any more often than ever, but they would have to explicitly address these ....

Deven McGraw – Center for Democracy & Technology – Director
I know we're close to reaching the end of our call so this is likely a discussion that's going to have to bleed into the next call, but does anybody have any thoughts on this? This would again be pursuing I think rather than focusing just on the matter of encryption at rest, it sounds like what Dixie's suggesting is that we look at the other addressable provisions in the security rule and specifically asking meaningful users to address how they're going to implement them.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Or at least this group, I think, should consider these, look at the list that we developed over a year ago, and we might even have changed our mind.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Any preliminary thoughts on that? All right, I propose that Paul and I will work to wordsmith the language that we did come up with on the encryption at rest point and we'll tee up this discussion as well. The other thing that we didn't get to today but we sure did get far is the issue of additional EHR security functionalities beyond those already required for stage one and some additional policies for patient

portals beyond the identification and authentication requirements that we've already teed up. That will be what we will focus on in the next call. Although, again, I would encourage all of you to take a look at how the recommendations on the portal issue are currently framed in the documents and either I'm inviting you to begin the discussion by e-mail so we can try to hone the issues. Or at least be as well prepared to discuss those points as you were today on all of the others, which really helped us to make a significant amount of progress.

Judy Faulkner – Epic Systems – Founder
Deven, I hate to back us up, but I at least should ask you whether we should. I asked one of our developers on the inpatient system to take a look at some of the things that were being proposed, and he brought up a couple of interesting things that maybe we should consider before we close the books on the stuff so far. One is on the provider authentication, and that is, we were thinking I think primarily of laptops that people use from their homes or other places. The two other really big things are the handhelds. So as you have a handheld and you are quickly trying to look up your patient's lab results are we going to get into a problem that two level authentication is going to make that too difficult? The other situation is the independent provider who works at three or four different hospitals and has to follow the progress of his or her patient at each of those hospitals having to get into each one, I think if it could be made simple, the two level authentication and just the second question asked, simple maybe not too hard. If it's going to require the person carrying multiple tokens around, that might be challenging.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

M
I'd like to suggest that it's a little more complex, even, because under certain circumstances the device itself can be considered a token. So I think it's important that we be careful not to accidentally rule out innovation and special consideration for those.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I think the other thing I want to make sure we do in that particular category is establish some areas that ONC would particularly ask questions about in rule making. Because, again, this is actually, to the extent that our recommendations are really aimed at NW-HIN, Nationwide Health Information Network governance, there's got to be a proposed rule on that, HHS has already let us know that, and so that means a broad opportunity for public comment on where this goes. One of the roles that we can play is teeing up specific questions that we might urge them to include, rather than trying to continually settle this issue. I feel like we've been over this a lot and each time we try to settle on it people bring up legitimate issues that ought to be pursued. Rather than continue to try to bring it up and settle it, I'm suggesting that we instead put these and identify them as things to be pursued in public comment. We'll work on wordsmithing that a little bit to make that more clear for folks to look at. But we're continually, I think, reminded of the challenges of trying to draw the line in the sand here, and it's hard.

Judy Faulkner – Epic Systems – Founder
I'm fine with that, Deven.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

M
I think an important thing you said is "specific questions." It feels a little bit less like kicking a can down the road that way.

Deven McGraw – Center for Democracy & Technology – Director
Yes, exactly. Not trying to push our responsibilities on to someone else.

M
Two smaller cans down the road.

Deven McGraw – Center for Democracy & Technology – Director
Agreed. Paul, did you have anything you wanted to add before we open to public comment?

Paul Egerman – Software Entrepreneur
No, good call.

Deven McGraw – Center for Democracy & Technology – Director
Great, thank you. Thanks, everybody. Okay, we're not done, we've got public comment. So, Judy, do you want to—?

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you check and see if anybody wishes to make a comment today?

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Thank you, everybody.

Deven McGraw – Center for Democracy & Technology – Director
Yes, thanks to all. Have a good weekend.

Judy Sparrow – Office of the National Coordinator – Executive Director
You, too. Goodbye.

W
Thanks ... I got caught up.

Deven McGraw – Center for Democracy & Technology – Director
Good.

W
... today.

Deven McGraw – Center for Democracy & Technology – Director
Excellent. Good luck next week.

W
Have a good weekend. Bye.